DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD, SUITE 2533
FT. BELVOIR, VIRGINIA 22060-6221

IN REPLY REFER TO CAN

JUL 14 1997

MEMORANDUM FOR DISTRIBUTION

SUBJECT: CIO Letter 97-3, Firewalls

This policy letter is directive in nature and its purpose is to provide interim guidance for the installation of DLA internet firewalls. Internet firewalls are devices or combinations of devices which, when placed between an external network and a local area network (LAN), enforce access control policies. This letter prescribes a strategy for reducing vulnerabilities of DLA networks and systems at the base level to risk of attack from external sources.

At a minimum and as resources permit, DLA activities will install firewalls at all points of connectivity between activity LANs and external networks, and will develop internal procedures necessary to ensure that access to network and system resources is restricted to authorized users.

Implementation of firewalls will require significant changes to network and system configurations, in particular, changes to network addresses of some systems and changes to dial-up access to LANs. As part of their pre-installation analysis, DSDC will determine specifics of these changes and will implement them in a gradual, coordinated process to minimize disruption to network users.

Firewall hardware and software will be centrally specified, installed, and integrated, but will be locally configured. CAN and CAAS will provide oversight with DSDC providing integration, installation, and technical support. Given the variety of functional and performance requirements at DLA activities, several different firewall configurations are anticipated. PLFA firewalls to be installed in FY97 will be based on the CheckPoint "Firewall-1" product, installed on Sun hardware. Additional configurations (e.g., for smaller sites) will be specified in future guidance. Activities which proceed with local firewall implementations prior to the issuance of such guidance will be required to transition to the standard configurations. Therefore, it would be prudent for those activities to coordinate early local firewall implementations with DSDC.

DLA-wide access policies will be supplemented by local access procedures developed by activity functional personnel and local Information System Security Officers (ISSOs) and approved by activity commanders. Local access procedures will reflect activity functional requirements and consequently will vary based on specific activity mission and function. The DLA-wide access policies which will be implemented as resources permit are as follows:

1. Firewalls shall be the sole points of entry and exit between DLA LANs and external systems and networks.

2. The basic posture of each firewall shall be to deny access except where expressly authorized. The date on which this rule is implemented shall be the date the firewall is considered to be fully operational. In the case of new firewalls, the target date for full operational status shall be 45 calendar days after installation.

3. Local configurations shall include one or more computing platforms external to the firewall, to be used to host applications and services such as inbound electronic mail, domain name system (DNS), the World Wide Web, File Transfer Protocol (FTP) and similar services requiring external access.

4. Local configurations shall position all dialup access external to the firewall.

5. Platforms located external to the firewall shall be considered to be exposed to increased risk and consequently
   (a) shall be limited to configurations recommended by DSDC and approved at the enterprise level,
   (b) shall be configured to disable all network services not expressly required for their operations,
   (c) shall have any security-related vendor software patches applied within 30 calendar days of notification by DSDC of patch availability, and
   (d) shall have their logs monitored on a continuous basis in order to detect attempted or actual intrusions. The initial configuration approved for use is HP/UX 9.X. (Additional configurations will be forthcoming.)

6. After a site is fully protected by firewalls, external access to platforms inside the firewall is prohibited, except where authentication/encryption is used. Initial mechanisms approved for use include: SecureID, Kerberos (version 5), and SecureRemote.

7. Access to external network services from platforms inside the firewall shall be channeled through proxy or similar concentrated servers where sessions can be logged and, as appropriate, restrictions or screens for viruses applied. Proxied services shall include: World Wide Web (HTTP), FTP, gopher, and WAIS. Concentrated services shall include mail post office services.

8. Connection of any modem or other base of external connectivity to a system or network inside the firewall, after a site is fully protected by firewalls, is prohibited and grounds for disciplinary action.

9. Activity commanders are responsible for notifying employees of this policy and enforcing adherence.

10. Temporary exceptions to this policy may be approved by activity commanders provided they are (a) specific and documented in writing, (b) limited in duration to 180 days or less, and (c) evaluated by local network and security staff prior to implementation. CANI, CAAS, and DSDC-TAC shall be notified within 24 hours when any such exceptions are granted. Transmission of details regarding exceptions should be via message traffic or secure electronic mail (ordinary electronic mail shall not be used).

All questions concerning this policy should be directed to either Carol Panneton, CANI, (703) 767-2198, DSN 427-2198, carol_panneton@hq.dla.mil, or Timothy Barb, CAASA, (703) 767-5434, DSN 427-5434, timothy_barb@hq.dla.mil.

Thomas Knapp

THOMAS J. KNAPP
Chief Information Officer
Defense Logistics Agency

DISTRIBUTION:

AQAC
CAAB
CAASA
CAHS
CANA
CANI
CANM
CANP
CANW
DASC-C
DASC-G
DASC-N
DSCC
DDRE
DDRW
DDSC-EA
DEUR
DFSC-S
DSCR-DD
DISC
DLMSO
DLSC
DNSC
DPAC
DPSC
DRMS-C
DSDC-A
DSDC-CI
DSDC-D
DSDC-E
DSDC-R
DSDC-T
FOX
MMP
MMBB
MMLZ